A STRONG LOWER BOUND ON FREE DISTANCE FOR PERIODIC CONVOLUTIONAL CODES

Daniel J. Costello, Jr.
Department of Electrical Engineering
Illinois Institute of Technology
Chicago, Ill. 60616

This is the manuscript of a 'long' paper to be presented at the 1970 IEEE International Symposium on Information Theory, Noordwijk, The Netherlands, June 15-19, 1970. (There will be no Proceedings or other publication of the papers submitted to this Symposium.)

This work was supported by the National Aeronautics and Space Administration (NASA Grant NGL 15-004-026) at the University of Notre Dame in liaison with the Flight Data Systems Branch of the Goddard Space Flight Center during the period during which the author was a research assistant under this grant.

ABSTRACT

A strong lower bound on the free distance of the class of non-systematic periodic time-varying convolutional codes is derived. This bound is then combined with other known bounds to show that more free distance is available with non-systematic codes than with systematic codes. Since it is known that free distance is a more important parameter than the conventional minimum distance for codes used with sequential decoding, it is argued that fewer decoding errors will be made with non-systmeatic codes than with systematic codes of the same rate and constraint length.

"A Strong Lower Bound on Free Distance for Periodic Convolutional Codes"

I. Introduction

It has recently been discovered that free distance is a more important parameter for convolutional codes used with sequential decoding than the conventional minimum distance [1]. Two important bounds on the free distance attainable with binary convolutional codes have been reported. McEliece and Rumsey [2] have shown a Plotkin-type upper bound on free distance for rate R = 1/N systematic convolutional codes. Asymptotically this bound states that

$$\lim_{m \to \infty} \frac{d_{FREE}}{n_A} < \frac{1-R}{2} , \tag{1}$$

where d_{FREE} is the free distance, m is the memory of the code, and $n_A = N(m+1)$ is the constraint length of the code. Neumann [3] has obtained a lower bound on free distance for non-systematic convolutional codes. Asymptotically this bound states that

$$\lim_{m \to \infty} \frac{d_{FREE}}{n_A} \geqq \begin{cases} 2H^{-1}(1-R) & \text{for } R \geqq 0.374 \\ \dfrac{2R\,(1-2^{2R-1})}{H(1-2^{2R-1}) + 2R-1} & \text{for } R \leqq 0.374 \end{cases} \tag{2}$$

where $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function. Note that for the range of rates above R = 0.374, this bound is twice the usual Gilbert lower bound on minimum distance. It is also known that the usual Gilbert lower bound holds for the free distance of systematic codes [2].

It is the purpose of this paper to prove a stronger lower bound than (2) for the more general class of non-systematic periodic time-varying convolutional codes. In particular, for this class of codes it will be shown that

$$\lim_{m \to \infty} \frac{d_{FREE}}{n_A} \geqq \frac{R(1-2^{R-1})}{H(1-2^{R-1}) + R-1} \quad . \tag{3}$$

Note that this bound is of the same form as the bound in (2) for $R \leqq 0.37$ ex:ept that 2R is replaced by R. It can also be shown that the upper bound in (1) holds for the class of systematic periodic time-varying codes [4].

The bounds of equations (1), (2), and (3) are plotted along with the usual Gilbert lower bound in Figure 1. Note that for the class of periodic codes the lower bound on non-systematic codes is everywhere greater than the upper bound on systematic codes. Hence more free distance is available from non-systematic periodic codes than from systematic periodic codes. The same conclusion can be drawn for the class of non-time-varying codes for the range of rates over which the lower bound on non-systematic codes exceeds the upper bound on systematic codes, i.e., for $R \leqq 0.374$.

These results have important implications when codes are being selected for use with sequential decoding. It has recently been shown that for various codes of a given constraint length used with sequential decoding, fewer decoding errors are made by the codes with larger free distances [1,5]. Therefore non-systematic codes will in general yield better sequential decoding performance than systematic codes. Bucher [6] has also arrived at this conclusion through an analysis of the sequential decoding algorithm.

II. Preliminaries.

The encoding equations for a rate R = k/N binary time-varying convolutional code can be written as

$$\underline{y} = \underline{x}\,\underline{G} \; , \tag{4}$$

where

$$\underline{x} = \left[\underline{x}_0, \underline{x}_1, \underline{x}_2, \ldots\right] = \left[\, x_0^{(1)} \ldots x_0^{(k)} \; x_1^{(1)} \ldots x_1^{(k)} \; X_2^{(1)} \ldots x_2^{(k)} \ldots \right] \tag{5}$$

is the sequence of binary information digits,

$$\underline{y} = \left[\underline{y}_0, \underline{y}_1, \underline{y}_2, \cdots \right] = \left[y_0^{(1)} \cdots y_0^{(N)} \; y_1^{(1)} \cdots y_n^{(N)} y_2^{(1)} \cdots y_2^{(N)} \cdots \right] \tag{6}$$

is the sequence of binary transmitted digits or codeword, and

$$\underline{G} = \begin{bmatrix} \underline{G}_0(0) & \underline{G}_1(0) & \underline{G}_2(0) & \cdots & \underline{G}_m(0) & \underline{0} & \underline{0} & \cdots \\ \underline{0} & \underline{G}_0(1) & \underline{G}_1(1) & \cdots & \underline{G}_{m-1}(1) & \underline{G}_m(1) & \underline{0} & \cdots \\ \underline{0} & \underline{0} & \underline{G}_0(2) & \cdots & \underline{G}_{m-2}(2) & \underline{G}_{m-1}(2) & \underline{G}_m(2) & \cdots \\ & & \ddots & & & & \ddots & \end{bmatrix} \tag{7}$$

is the semi-infinite generator matrix in which each

$$\underline{G}_h(u) = \begin{bmatrix} g_{h1}^{(1)}(u) & g_{h1}^{(2)}(u) & \cdots & g_{h1}^{(N)}(u) \\ g_{h2}^{(1)}(u) & g_{h2}^{(2)}(u) & \cdots & g_{h2}^{(N)}(u) \\ \vdots & \vdots & & \vdots \\ g_{hk}^{(1)}(u) & g_{hk}^{(2)}(u) & \cdots & g_{hk}^{(N)}(u) \end{bmatrix} \tag{8}$$

is a k x N matrix of binary digits, $0 \leqq h \leqq m$, $0 \leqq u < \infty$.
$\underline{x}_i = \left[x_i^{(1)} \; x_i^{(2)} \; \cdots \; x_i^{(k)} \right]$ is the block of k input digits into the encoder at time unit i and $\underline{y}_i = \left[y_i^{(1)} \; y_i^{(2)} \; \cdots \; y_i^{(N)} \right]$ is the block of N output digits from the encoder at time unit i. m is called the memory of the code and $n_A = N(m+1)$, the maximum number of transmitted digits which can be affected by a single non-zero block of information digits, is called the constraint length.

If

$$\underline{G}_h(u) = \underline{G}_h(u+T), \quad 0 \leqq h \leqq m, \quad 0 \leqq u < \infty, \tag{9}$$

then the time-varying code is periodic with period T, i.e., the generator matrix repeats itself every kT rows. If T = 1, every set of k rows in $\underline{G}$

is the same (except for shifting N columns to the right), and the code is non-time-varying or fixed.

Let $\underline{x}^{(j)} = \left[x_0^{(j)}\ x_1^{(j)}\ x_2^{(j)} \ldots \right]$ be the $j^{\underline{th}}$ information subsequence, $1 \leqq j \leqq k$, and $\underline{y}^{(j)} = \left[y_0^{(j)}\ y_1^{(j)}\ y_2^{(j)}\ \ldots \right]$ be the $j^{\underline{th}}$ transmitted subsequence, $1 \leqq j \leqq N$. Then if the first k transmitted subsequences are exact reproductions of the k information subsequences, the code is said to be in systematic form. Clearly this places the following restrictions on the generator matrix of a periodic code:

$$\underline{G}_0 (u) = \left[I_k : \underline{Q}_0 (u) \right], 0 \leqq u < T, \tag{10}$$

where I_k is the k x k identity matrix and $\underline{Q}_0$ (u) is a k x (N-k) matrix of binary digits, and

$$\underline{G}_h (u) = \left[0_k : \underline{Q}_h (u) \right], \ 0 \leqq u < T, \ \ 1 \leqq h \leqq m, \tag{11}$$

where 0_k is the k x k all-zero matrix and $\underline{Q}_h$ (u) is a k x (N-k) matrix of binary digits.

The free distance of a convolutional code is defined as the minimum Hamming distance between any two distinct codewords, i.e.,

$$d_{FREE} = \min_{\underline{x} \neq \underline{x}'} d_H (\underline{x}\ \underline{G}, \underline{x}'\ \underline{G}), \tag{12}$$

where $d_H (\cdot\ , \cdot)$ denotes the Hamming distance between the two arguments. Because the encoding process is linear, (12) can be simplified to

$$d_{FREE} = \min_{\underline{x} \neq \underline{0}} W_H (\underline{x}\ \underline{G}), \tag{13}$$

where $W_H(\cdot)$ denotes the Hamming weight of the argument. Hence d_{FREE} is seen to be the minimum Hamming weight codeword.

For all codes that do not exhibit catastrophic error propagation, Massey [7] has shown that infinitely long information sequences must produce infinite weight codewords. Therefore the minimum free weight codeword must be produced by a finite length information sequence. In fact it is known that this length cannot be more than the order of m^2 for systematic R = 1/N fixed codes [1,8]. A similar bound can be shown to hold for almost all non-systematic periodic codes [4]. Let L be the bound on the length (in blocks of k digits each) of information sequence needed to produce the minimum free weight codeword. Henceforth we will consider only non-systematic periodic codes with period $T \geq L + m$ such that T is only an algebraic function of m, i.e., T grows less than exponentially with m. This is equivalent to expurgating from the ensemble of codes that vanishingly small fraction of codes for which L may grow exponentially with m.

III. Three Lemmas.

Lemma 1. No information sequence with a string of m or more consecutive all-zero blocks can produce the minimum free weight codeword.

Proof. Following any information sequence with a string of m or more consecutive all-zero blocks and then additional non-zero blocks can only add to the weight of the codeword. Hence such an information sequence cannot produce the minimum free weight codeword. Q.E.D.

Let S_h be the set of all information sequences of length h (in blocks of k digits each) such that $\underline{x}_u \neq \underline{0}$, $\underline{x}_{u+h-1} \neq \underline{0}$, $\underline{x}_0 = \underline{x}_1 = \dots = \underline{x}_{u-1} = \underline{x}_{u+h} = \underline{x}_{u+h+1} = \dots = \underline{0}$, for some u, $0 \leq u < T$, and which contain no string of m or more consecutive all-zero blocks inclusive between block u and block u+h-1. Now let F(h,d) be the fraction of codes with a codeword of weight d or less produced by an information sequence from the set S_h.

Lemma 2.

$$F(1,d) \leq \frac{T(2^k-1) \sum_{j=0}^{d} \binom{N(m+1)}{j}}{2^{N(m+1)}} .$$

Proof. For a particular information sequence of length 1 belonging to S_1, we must specify the number of different ways of choosing a low weight row of $\underline{G}$. Clearly, there are $\sum_{j=0}^{d} \binom{N(m+1)}{j}$ ways of choosing a low weight $N(m+1)$ - tuple. Once one row of $\underline{G}$ has been specified as having low weight, the $\left[k-1 + (T-1)k \right] N(m+1) = TkN(m+1) - N(m+1)$ digits in the remaining distinct rows can be chosen arbitrarily. Hence a particular information sequence from S_1 can produce a low weight codeword in at most $2^{TkN(m+1) - N(m+1)} \sum_{j=0}^{d} \binom{N(m+1)}{j}$ codes. Since there are $T(2^k-1)$ ways of choosing such an information sequence and since there are approximately $2^{TkN(m+1)}$ total codes in the expurgated ensemble,

$$F(1,d) \leqq \frac{T\,(2^k-1) \sum_{j=0}^{d} \binom{N(m+1)}{j}}{2^{N(m+1)}} . \qquad \text{Q.E.D.}$$

Lemma 3.

$$F(h,d) \leqq \frac{T\,(2^k-1)^2 \sum_{j=0}^{d} \binom{N(m+h)}{j}}{2^{(N-k)h}\ 2^{2k + Nm}} \qquad \text{for } h = 2, 3, \ldots, L.$$

Proof. For a particular information sequence of length h belonging to S_h, the transmitted sequence contains m+h blocks. Hence there are $\sum_{j=0}^{d} \binom{N(m+h)}{j}$ low weight transmitted sequences. If the information sequence being considered is one for which u = 0, then the encoding equations can be written as follows:

$$\begin{aligned}
\underline{y}_0 &= \underline{x}_0\, \underline{G}_0\ (0) \\
\underline{y}_1 &= \underline{x}_1\, \underline{G}_0\ (1) + \underline{x}_0\, \underline{G}_1\ (1) \\
\underline{y}_2 &= \underline{x}_2\, \underline{G}_0\ (2) + \underline{x}_1\, \underline{G}_1\ (2) + \underline{x}_0\, \underline{G}_2\ (2) \\
&\vdots \\
\underline{y}_m &= \underline{x}_m\, \underline{G}_0\ (m) + \underline{x}_{m-1}\, \underline{G}_1\ (m) + \ldots + \underline{x}_0\, \underline{G}_m\ (m) \qquad (14) \\
&\vdots \\
\underline{y}_{h-1} &= \underline{x}_{h-1}\, \underline{G}_0\ (h-1) + \underline{x}_{h-2}\, \underline{G}_1\ (h-1) + \ldots + \underline{x}_{h-m-1}\, \underline{G}_m\ (h-1) \\
&\vdots \\
\underline{y}_{m+h-1} &= \underline{x}_{h-1}\, \underline{G}_m\ (m+h-1).
\end{aligned}$$

Since no information sequences with a string of m or more consecutive all-zero blocks belong to S_h, and since $T \geqq m+h$, equations (14) are a linearly independent set. Therefore, given a particular information sequence from S_h with $u = 0$ and a particular low weight transmitted sequence, there are $2^{TkN(m+1) - N(m+h)}$ solutions to equations (14). Since there are at most $T2^{k(h-2)} (2^k-1)^2$ different information sequences in S_h, and since there are approximately $2^{TkN(m+1)}$ total codes in the expurgated ensemble,

$$F(h,d) \leqq \frac{T(2^k-1)^2 \sum_{j=0}^{d} \binom{N(m+h)}{j}}{2^{h(N-k)}\ 2^{2K + Nm}} \quad \text{for } h = 2,3,\ldots, L. \quad \text{Q.E.D.}$$

IV. Derivation of the Bound.

Theorem 1. There exists at least one non-systematic periodic convolutional code such that

$$\lim_{m\to\infty} \frac{d_{FREE}}{n_A} \geqq \frac{R(1-2^{R-1})}{H(1-2^{R-1})+R-1} .$$

Proof. From lemma 1 and the fact that no information sequence of length greater than L can produce the minimum free weight codeword, if $\sum_{h=1}^{L} F(h,d) < 1$, then there exists at least one code with $d_{FREE} > d$. Let $F_{max} = \max_{1 \leqq h \leqq L} F(h,D)$. Then if $LF_{max} < 1$, there exists at least one code with $d_{FREE} > d$.

First an upper bound $\overline{F}_{max}$ on F_{max} will be obtained. Since $\sum_{j=0}^{d} \binom{N(m+h)}{j} \leqq 2^{N(m+h)\, H(\frac{d}{N(m+h)})}$, an upper bound on F_{max} can be obtained by maximizing $N(m+h)\, H(\frac{d}{N(m+h)}) - h(N-k)$. Let h_{max} be the value of h which maximizes this expression. By setting its derivative with respect to h equal to zero and solving for h, it can be shown that $h_{max} = \frac{d}{N(1-2^{R-1})} - m$.

$$\text{Hence } F_{max} \leqq \overline{F}_{max} = \frac{T(2^k-1)^2}{2^{2k + Nm}} \cdot 2^{\frac{d}{1-2^{R-1}} H(1-2^{R-1}) - h_{max}(N-k)} .$$

Therefore if $\overline{LF}_{max} < 1$, then $LF_{max} < 1$ and there exists at least one code with $d_{FREE} > d$. Alternatively, if d is the least integer such that $\overline{LF}_{max} \geqq 1$, then there exists at least one code with $d_{FREE} \geqq d$.

Hence we must find the least integer d such that $\log_2 LT + 2 \log_2 (2^k-1) + \frac{d}{1-2^{R-1}} H(1-2^{R-1}) - h_{max}(N-k) \geqq 2k + Nm$. Dividing by m and dropping all terms which approach zero as m approaches infinity, we obtain $\frac{d}{m} (\frac{H(1-2^{R-1})}{1-2^{R-1}}) - \frac{d}{m} (\frac{1-R}{1-2^{R-1}}) + (N-k) \geqq N$. This implies that $\frac{d}{m} \geqq \frac{K(1-2^{R-1})}{H(1-2^{R-1}) + R-1}$. Therefore there exists at least one code such that

$$\lim_{m\to\infty} \frac{d_{FREE}}{n_A} \geqq \frac{R(1-2^{R-1})}{H(1-2^{R-1}) + R-1} \text{ . Q.E.D.}$$

This bound is interesting in itself in that it is the strongest lower bound known on any class of convolutional codes. This is due to the fact that we are bounding d_{FREE}, which is always at least as great as the conventional minimum distance[1], and we are expanding the class of codes to include non-systematic periodic codes. Table 1 shows the ratio of the bound in theorem 1 to the usual Gilbert lower bound as a function of rate. For instance at R = ½, the bound of theorem 1 is approximately 3½ times as strong as the Gilbert bound. Note that for very low rates, the two bounds are almost the same since only slight gains in d_{FREE} can be expected from non-systematic codes over systematic codes. However at very high rates, non-systematic codes offer great improvements in d_{FREE} over systematic codes and the ratio of the bounds is quite large.

V. Conclusions.

The objective of this paper was to demonstrate that more free distance is available from non-systematic codes than from systematic codes. The bound of theorem 1 along with equation (1) shows that this is true for periodic codes of all rates. Equations (1) and (2) indicate that this is true for fixed codes with $R \leq 0.374$. Since this is the range of rates for which the least improvement would be expected, tighter bounding arguments should produce the same result for fixed codes of all rates.

Since free distance is closely related to sequential decoding probability of error, these results indicate the desirability of using non-systematic codes with sequential decoding.

VI. Acknowledgements

The author wishes to thank Professor James L. Massey of the University of Notre Dame for his constant help and guidance during the course of this research. Graditude is also due to the National Aeronautics and Space Administration for supporting this work under NASA Grant 15-004-026.

VII. References.

1. Costello, D. J., "A Construction Technique for Random-Error-Correcting Convolutional Codes", IEEE Transactions, Vol. IT-15, pp. 631-636 (1969).

2. McEliece, R. and H. Rumsey, "Capabilities of Convolutional Codes", Jet Propulsion Laboratory SPS 37-50, Vol. 3 (1968).

3. Neumann, B., "Distance Properties of Convolutional Codes", M.S. Thesis, Department of Electrical Engineering, Mass. Inst. of Tech. (Cambridge, Mass., 1968).

4. Costello, D. J., "Construction of Convolutional Codes for Sequential Decoding", Univ. of Notre Dame Tech. Rept. EE 692 (1969).

5. Jelinek, F. and L. R. Bahl, "Maximum Likelihood and Sequential Decoding of Short Constraint Length Convolutional Codes", paper presented at the Allerton Conference on Circuit and System Theory (Monticello, Ill., 1969).

6. Bucher, E. A., "Error Mechanisms for Convolutional Codes", Ph.D. Thesis, Dept. of Electrical Engineering, Mass. Inst. of Tech. (Cambridge, Mass., 1968).

7. Massey, J. L., "Catastrophic Error-Propagation in Convolutional Codes", paper presented at the Midwest Symposium on Circuit Theory (Notre Dame, Ind., 1968).

8. Miczo, A. and L. D. Rudolph, "A Note on the Free Distance of a Convolutional Code", IEEE Transactions Information Theory, in press (1969).

TABLE 1

RATE	λ'/λ
0	1
.05	1.33
.10	1.53
.15	1.71
.20	1.90
.25	2.12
.30	2.34
.35	2.58
.40	2.86
.45	3.20
.50	3.57
.55	4.03
.60	4.62
.65	5.30
.70	6.25
.75	7.60
.80	9.40
.85	12.37
.90	18.15
.95	32.85
1	1

$\lambda' = \dfrac{R(1-2^{R-1})}{H(1-2^{R-1}) + R-1}$ is the bound of theorem 1.

$\lambda = H^{-1}(1-R)$ is the usual Gilbert lower bound.

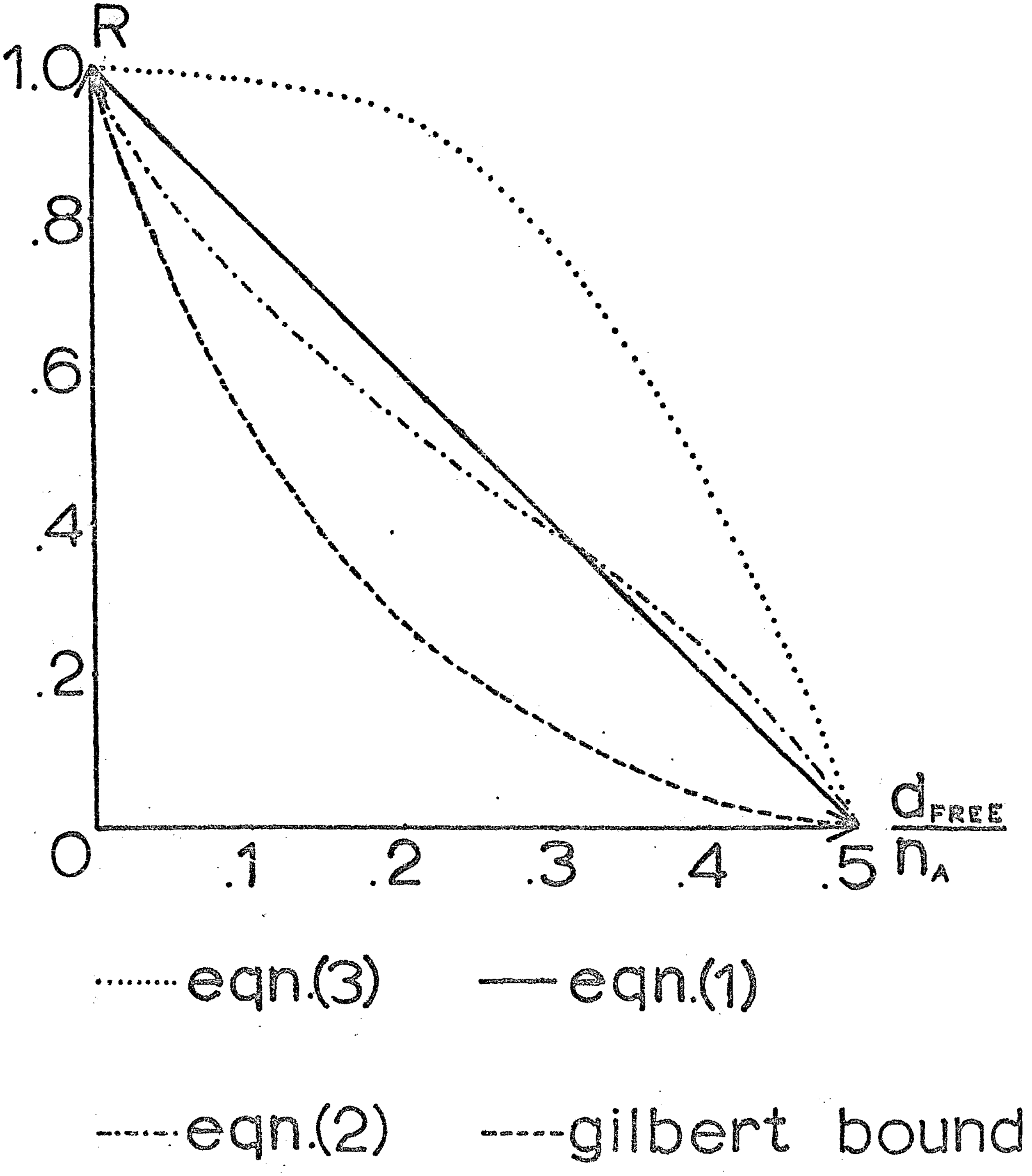

FIGURE 1.